Aizsardzības ministrija

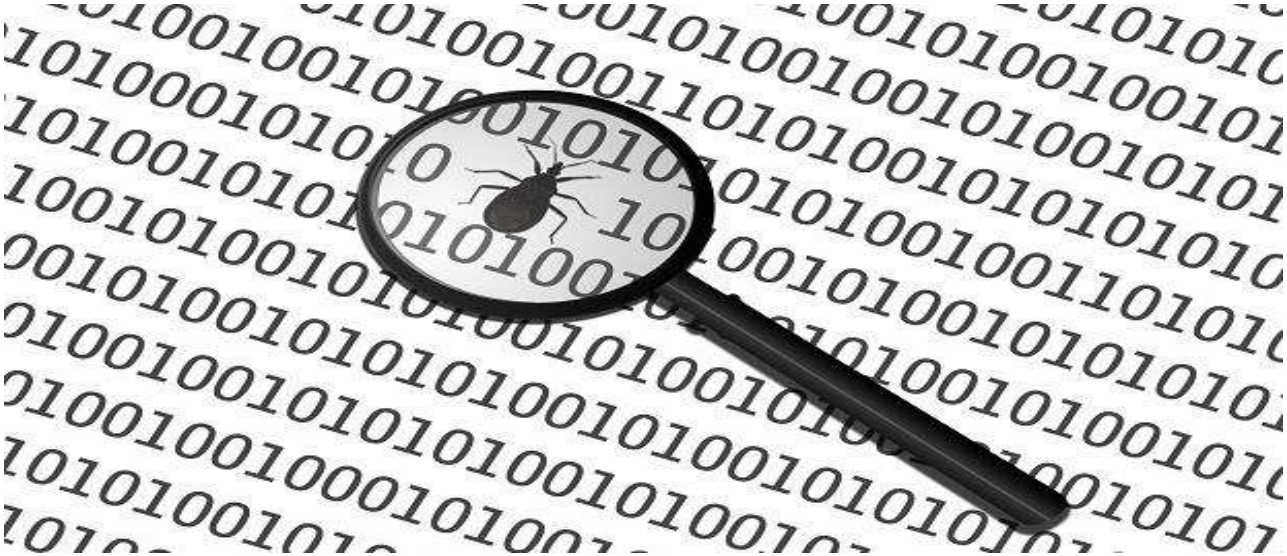
Atbildīga ievainojamību atklāšana

Ieva Ilvesa,
Aizsardzības ministrijas
Nacionālās kiberdrošības politikas koordinācijas nodaļas vadītāja

CERT.LV IT drošības seminārs «Esi drošs», 2016.gada 26.aprīlī

Aizsardzības ministrija

Atbildīga ievainojamību atklāšanas politika nosaka kārtību kādā ikviens var ziņot par informācijas sistēmās atrastām nepilnībām – ievainojamībām un atspoguļo iesaistīto pušu tiesības un pienākumus, veicot ievainojamību atklāšanu un to novēršanu.



Aizsardzības ministrija

Politikas mērķis un nepieciešamība

- **Stiprināt drošību** komplicētā virtuālā vidē
- Atklāt un **mazināt esošās ievainojamības,** to ļaunprātīgu izmantošanu
- **Iesaistīt pētniekus** un augstas kvalifikācijas speciālistus valsts kiberdrošības uzlabošanai
- Veicināt iesaistīto pušu tiesisko aizsardzību
- **Veicināt interesi un izpratni** par kiberdrošību

Aizsardzības ministrija

Kas ir atbildīga ievainojamību atklāšana?

Iesaistītās puses

1)Resursu turētāji

2) Pētnieki, ētiskie hakeri, lietotāji

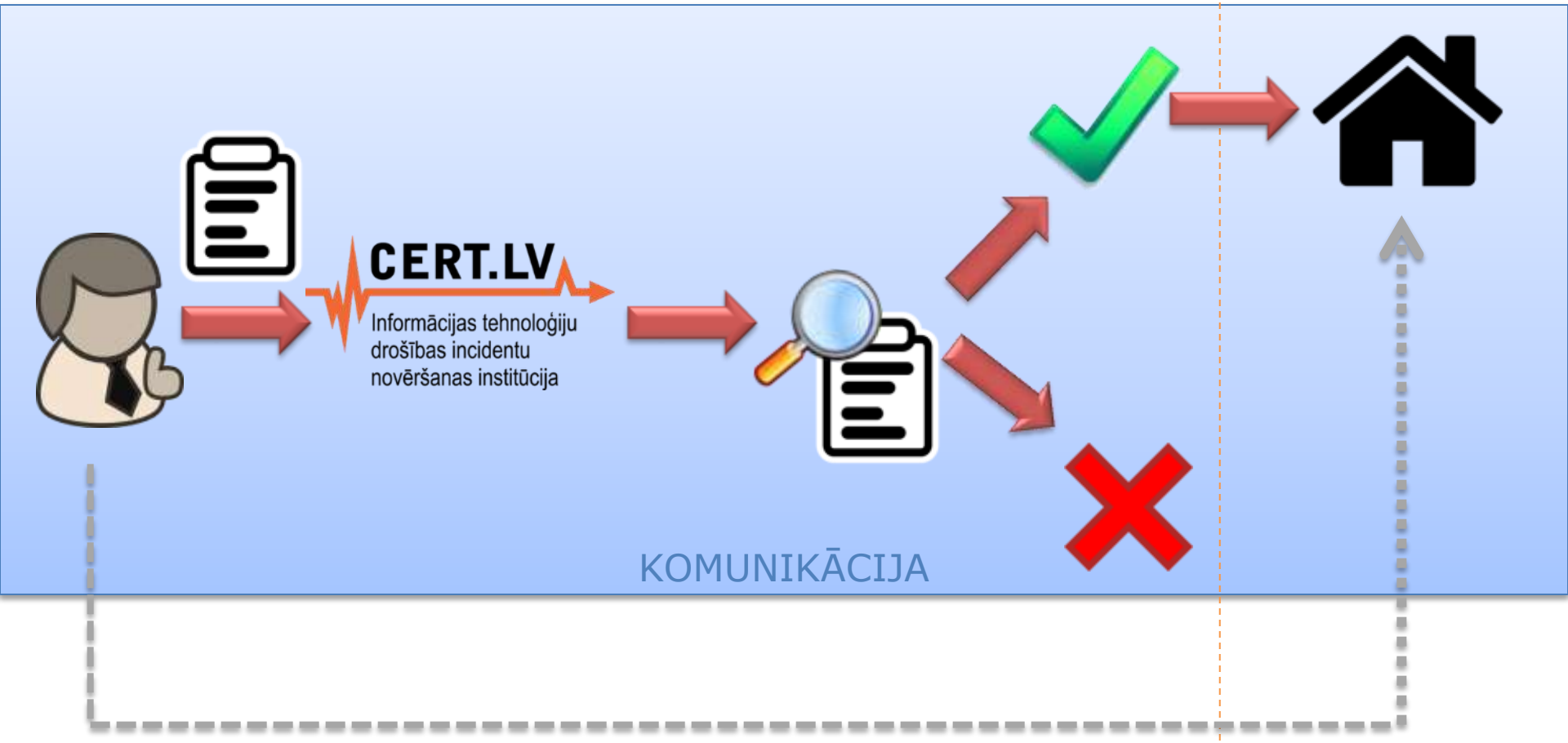
Procesa elementi

1) Ziņošana
2) Koordinācija

3) Novēršana
4) Publiskošana

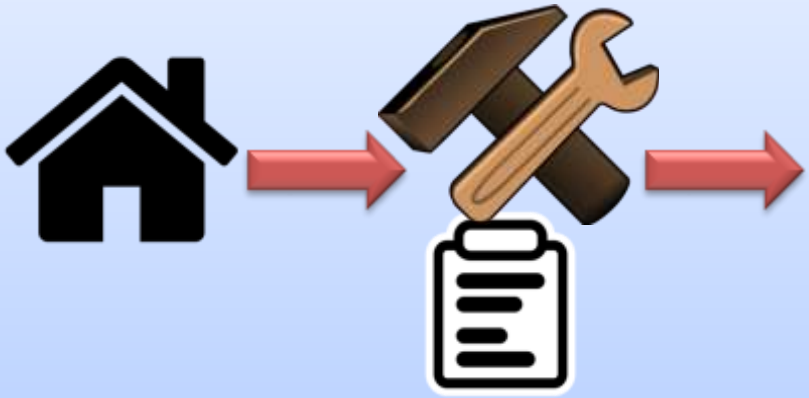
Aizsardzības ministrija

Procesa kārtība



Aizsardzības ministrija

Procesa kārtība



CERT.LV

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

KOMUNIKĀCIJA

Aizsardzības ministrija

Procesa nosacījumi

Resursa turētājam

- **Novērst** ievainojamības
- **Neiesūdzēt** tiesā
- **Ievērot** termiņus
- Noteikt **komunikācijas** mehānismus
- **Publicēt** pēc novēršanas
- Pateicība?

Ziņotājam

- Meklēt tikai **minimālos** pierādījumus
- Ziņot **laicīgi** un drošā veidā
- **Nepublicēt** pirms novēršanas
- **Neveikt** sociālās inženierijas, DDOS **uzbrukumus**

Aizsardzības ministrija

Integrēšana IT drošības likumā

- Likuma 6.1.panta esošā redakcija par drošības nepilnībām nosaka:
  - tās novērst, ja atklāj pati iestāde vai CERT.LV;
  - tās novērst 90 dienu laikā.

- Tiks papildināts ar rīcību, ja drošības nepilnību konstatē trešā puse (persona)

  - Papildus tiks izstrādāti MK noteikumi, lai atrunātu precīzi:
  - informāciju, kas ir ziņojumā;
  - minimālo pierādījumu kopumu;
  - komunikācijas aspektus.

Aizsardzības ministrija

Grozījumi Krimināllikumā

241.pants. Patvaļīga piekļūšana automatizētai datu apstrādes sistēmai

(1) **Par patvaļīgu piekļūšanu** automatizētas datu apstrādes sistēmas resursiem, ja tas saistīts ar sistēmas aizsardzības līdzekļu pārvarēšanu vai ja tas izdarīts bez attiecīgas atļaujas vai izmantojot citai personai piešķirtas tiesības un ja ar to radīts būtisks kaitējums, —
soda ar brīvības atņemšanu uz laiku līdz diviem gadiem vai ar īslaicīgu brīvības atņemšanu, vai ar piespiedu darbu, vai ar naudas sodu.

(2) [..]

(3) Par šā panta pirmajā daļā paredzētajām darbībām, ja tās izraisījušas smagas sekas vai **ja tās vērstas pret automatizētu datu apstrādes sistēmu, kas apstrādā informāciju, kura saistīta ar valsts politisko, ekonomisko, militāro, sociālo vai citu drošību**, —
soda ar brīvības atņemšanu uz laiku līdz pieciem gadiem vai ar īslaicīgu brīvības atņemšanu, vai ar piespiedu darbu, vai ar naudas sodu, konfiscējot mantu vai bez mantas konfiskācijas.

Aizsardzības ministrija

Izaicinājumi

- Kārtības un nosacījumu ievērošana
- Resursa turētāju nespēja adekvāti reaģēt uz ziņojumiem
- Komunikācija
- Laicīga ievainojamību novēršana
- Priekšstatu, stereotipu maiņa par ievainojamību meklēšanu
- Apjomīgs skaidrojošais darbs, lai visiem būtu skaidra izpratne

→ Riski ir un tie būs pastāvīgi… bet ieguvumi ir daudz lielāki

Aizsardzības ministrija

Starptautiskā pieredze

- **Starptautiskās kompānijas:**
  - **Google**: Vulnerability Reward Program
  - **Microsoft**: Coordinated Vulnerability Disclosure
  - **Facebook**
- **ISO/IEC 29147, ISO/IEC 30111**
- **www.bugcrowd.com**
- **Nīderlandes valdība**

Aizsardzības ministrija

Nīderlandes Nacionālais kiberdrošības centrs jeb NCSC

- Reaģē uz iesniegtajiem ziņojumiem
- Starpnieks ziņotājam un organizācijai (ja nepieciešams)
- Atbalsta un sekmē atbildīgas ievainojamību atklāšanas procesa ieviešanu

Aizsardzības ministrija

NL prokurora atbalsta paziņojums

"Whenever a hacker gets in touch directly and safely with the owner of the IT-system regarding a discovered vulnerability and no data is manipulated or removed then there may be a case of RD. This means there is no reason for a criminal investigation and for a criminal prosecution"

Aizsardzības ministrija

Pieredze Latvijā

- Swedbank
- Vairāki atsevišķi gadījumi CERT.LV pieredzē:
  - Valmieras pašvaldības hakatons
  - Banku autentifikācija
  - Vairākas valsts un pašvaldību mājas lapas un informācijas sistēmas
  - Mobilās lietotnes
  - «Rīgas satiksmes» mobilā lietotne

Aizsardzības ministrija

Paldies!

Ieva Ilvesa,
Aizsardzības ministrijas
Nacionālās kiberdrošības politikas koordinācijas nodaļas vadītāja

CERT.LV IT drošības seminārs «Esi drošs», 2016.gada 26.aprīlī